



Vantaan kaupungin tietoturva- ja tietosuojapolitiikka



VANTAAN KAUPUNGINHALLITUS 28.05.2018

Sisällysluettelo

1	Tietoturva- ja tietosuojapolitiikan perusta.....	3
2	Kaupungin tietoturvan ja tietosuojan tavoitteet.....	3
2.1	Tietoturvatavoitteet.....	3
2.2	Tietosuojatavoitteet.....	4
3	Tietoturva- ja tietosuojariskeihin varautuminen.....	5
3.1	Tietoriskien arvioiminen.....	5
3.2	Riskienhallinnan toimenpiteet.....	7
4	Tietoturvan ja tietosuojan vastuut ja organisointi.....	8
4.1	Tietoturvan ja tietosuojan tilivelvollisuudet ja vastuut.....	8
4.1.1	Kaupunginhallitus ja kaupunginjohtaja.....	8
4.1.2	Apulaiskaupunginjohtajat.....	9
4.1.3	Vantaan tytäryhtiöiden ja liikelaitosten päättäjät.....	9
4.1.4	Tulosalueiden johtajat ja tulosyksiköiden päälliköt sekä muut esimiehet.....	9
4.1.5	Kaupungin palveluiden päälliköt ja vastuulliset.....	10
4.1.6	Palveluntoimittajat.....	10
4.1.7	Tiedon omistajat.....	11
4.1.8	Henkilörekisterin pitäjät.....	11
4.1.9	Tietojärjestelmien omistajat.....	11
4.1.10	Työntekijöiden ja muiden tietoja käsittelevien vastuu.....	12
4.2	Tietoturvan ja tietosuojan järjestäminen: tietoturvan ja tietosuojan hallinta, -palvelu ja -teknologia.....	13
4.2.1	Tietoturvapäällikkö.....	13
4.2.2	Tietosuojavastaava.....	14
4.2.3	Tietoturva- ja tietosuojatyöryhmä.....	14
4.2.4	Toimialojen tietoturva- ja/tai tietosuojavastaavat.....	14
4.2.5	Tietohallinnon palvelukeskus.....	15
4.2.6	Henkilöstökeskus.....	15
4.2.7	Hankintakeskus ja hankinnoista vastaavat.....	15
5	Tietoturvan ja tietosuojan seuranta, koulutus, ohjeet ja viestintä.....	16
6	Liite 1: Tietoturvan ja tietosuojan käsitteitä.....	17

1 Tietoturva- ja tietosuojapolitiikan perusta

Tietoturva- ja tietosuojapolitiikka sisältää tavoitteet, periaatteet, vastuut ja toimintatavat, jotka ohjaavat Vantaan kaupungin toimintaa kaupungin tietojen käsittelyssä ja suojaamisessa. Tietoturva- ja tietosuojapolitiikan tavoitteena on varmistaa yhdenmukaiset käytännöt tietoturvan ja tietosuojan toteuttamiseksi. Tietoturvasta ja tietosuojasta huolehtiminen on osa kaupungin riskienhallintaa. Kaikessa tietojen käsittelyssä noudatetaan lainsäädäntöä, viranomaismääräyksiä ja -ohjeita sekä kaupungin määräyksiä, ohjeita ja linjauksia.

Tietoturva- ja tietosuojapolitiikka koskee Vantaan kaupungin johtoa, luottamushenkilöitä, viranhaltijoita, henkilöstöä, konsultteja sekä muita kaupungin tietoja käsitteleviä henkilöitä. Se tulee huomioida myös kaupungin käyttämien palvelutuottajien ja sidosryhmien sekä kaupunkikonsernin tytäryhtiöiden toiminnassa. Tietoturva- ja tietosuojapolitiikkaa täydentävät kaupungin yleiset tietoturva- ja tietosuojaohjeet sekä toimialojen omat tarkentavat tietoturva- ja tietosuojaohjeet.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Asiakirjan sisältöä tarkistetaan ja päivitetään säännöllisesti. Asiakirja on julkinen.

2 Kaupungin tietoturvan ja tietosuojan tavoitteet

Kaupungin tietoturvan ja tietosuojan yleistavoite on

Oikea tieto oikeilla ihmisillä oikeassa paikassa oikeaan aikaan!

2.1 Tietoturvatavoitteet

Vantaan kaupunki huolehtii tietojen, asiakirjojen ja tietojärjestelmien saatavuudesta, käytettävyydestä, eheydestä ja suojaamisesta sekä muusta tiedon laatuun vaikuttavista tekijöistä. Samoin kaupunki huolehtii riskiarvioon perustuvien tarpeellisten organisatoristen ja teknisten toimenpiteiden suorittamisesta tietojen suojaamiseksi, kuten asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta tai siirtämiseltä.

Tiedon suojaaminen on oleellinen osa kaupungin kokonaisturvaa ja päivittäistä toimintaa sekä tärkeä osa kaupungin toiminnan ja palveluiden laatua ja varmentamista. Kaupungin hallussa olevat tiedot ja tietojen käsittely sekä tietojärjestelmät ja -verkot suojataan lainsäädännön edellyttämällä tavalla kaikissa olosuhteissa, jotta toiminnan laatu ja jatkuvuus pystytään varmistamaan.

Vantaan kaupungin tietoturvatavoitteet ovat:

- Tietoriskien ennakointi ja vaikutusten järjestelmällinen hallitseminen jatkuvalla tietoriskien tunnistamisella, arvioimisella ja toimenpiteillä
- Tiedon ja tietolähteiden luotettavuuden, virheettömyyden ja laadun varmistaminen kaupungin johtamisessa, päätöksenteossa, toiminnassa ja viestinnässä
- Tiedon saatavuuden ja käytettävyyden varmistaminen
- Tiedon ja tietojärjestelmien valtuudettoman tai oikeudettoman käytön estäminen
- Tiedon tahattoman tai tahallisen tuhoutumisen tai vääristymisen estäminen
- Toiminnan keskeyttävien häiriöiden estäminen ja toipumiseen varautuminen
- Tietoturvaloukkauksien havaitseminen, jäljittäminen, tutkinta ja niistä toipuminen
- Sähköisen asioinnin saatavuuden, luotettavuuden ja kiistämättömyyden varmistaminen
- Kaupungin tietoturvapoliittikan ja -periaatteiden noudattamisen varmistaminen kaupungin käyttämissä tietopalveluissa ja tietojärjestelmissä
- Kaupungin tärkeiden palveluiden ja prosessien keskeytymättömän toiminnan suojaaminen ja häiriöihin varautuminen mukaan lukien tietojärjestelmät ja -verkot
- Tietoturva huomioidaan kaupungin ja eri osapuolten välisissä sopimuksissa
- Valtionhallinnon tietoturvaperiaatteiden perustietoturvatason ja kriittisissä toiminnoissa korotetun tietoturvatason (VAHTI) saavuttaminen ja toteuttaminen.

Tietoturvatavoitteiden saavuttaminen edellyttää kaupungin kaikkien toimialojen osalta sitoutunutta ja määrätietoista toteutusta.

2.2 Tietosuojatavoitteet

Vantaan kaupunki noudattaa asiakkaiden, kuntalaisten ja kaupungin henkilöstön henkilötietojen keräämisessä ja käsittelyssä voimassa olevaa lainsäädäntöä ja seuraavia tietosuojatavoitteita.

Vantaan kaupungin tietosuojatavoitteet ovat:

- Lain ja kaupungin ohjeiden noudattaminen varmistetaan henkilötietojen käsittelyn suunnittelulla ja osoitetaan dokumentoinnilla.
- Tietosuojasta huolehditaan henkilötietojen käsittelyn koko elinkaaren ajan:
 - Hallinnollisilla ja teknisillä toimenpiteillä varmistetaan, että käsittelyyn valitaan vain käyttötarkoituksen kannalta tarpeelliset henkilötiedot.
 - Henkilötietoja kerätään ja käsitellään vain tiettyä etukäteen määriteltyä ja lain mukaisesti perusteltua tarkoitusta varten.
 - Henkilötietoja ei käsitellä kauemmin kuin on tarpeen niiden käyttötarkoituksen vuoksi.
 - Vain lain velvoittamat ja kaupungin ohjeiden mukaiset henkilötiedot arkistoidaan käsittelytarpeen päätyttyä.
 - Henkilötiedot hävitetään lainmukaisen säilytysajan päätyttyä kaupungin ohjeistuksen mukaisesti.
- Varmistetaan henkilöstön ja sidosryhmien pääsy henkilötietoihin vain tehtävien edellyttämällä oikeudella ja tavalla.
- Henkilötietojen käsittelyssä huolehditaan tietojen virheettömyydestä.
- Henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen toteutetaan kaupungilla hallinnollisilla ja teknisillä toimenpiteillä.
- Tietosuoja huomioidaan kaupungin ja eri osapuolten välisissä sopimuksissa.

Tietoturvan ja tietosuojan käsitteitä on määritelty *liitteessä 1: Tietoturvan ja tietosuojan käsitteitä*.

3 Tietoturva- ja tietosuojariskeihin varautuminen

3.1 Tietoriskien arvioiminen

Tietoturva- ja tietosuojatoimenpiteitä suunniteltaessa ja kehitettäessä tulee arvioida ja analysoida toimintaan liittyvät tietoriskit ja tietosuojariskit. Tietoriskien ja tietosuojariskien suuruuden perusteella voidaan määrittää optimaaliset hallinnolliset ja tekniset tietoturva- ja tietosuojavaatimukset toimintaa suojaaviksi toimenpiteiksi.

Kaupungin tiedon määrä on valtava, joten sen hallitseminen on haasteellista. Tieto voi olla yksittäisessä asiakirjassa, sähköposti-, pika- tai tekstiviestissä, anturissa, verkossa, pilvipalvelussa, tietokannassa, tietokoneen tai puhelimen muistissa, ääni- tai kuvatiedostossa tai ihmisen muistissa tai paperilla.

Tietoriskejä tulee arvioida ja hallita kaupungin riskienhallinnan ohjauksen mukaisesti ja suurimmat tietoturva- ja tietosuojariskit tulee sisältyä organisaation tai palvelun riskienhallintasuunnitelmaan ja jatkuvaan riskien arviointiin.

Tietoon kohdistuu tyypillisesti seuraavia riskejä:

- Tietoon pääsy on hankalaa, hidasta tai estetty (saatavuus).
- Tieto vuotaa sivullisille (luottamuksellisuus).
- Tieto ei ole käyttökelpoista puutteen/virheen vuoksi tai tieto on hävinnyt (tarkkuus).
- Tieto ei jalostu eikä ole käyttökelpoista toiminnan kehityksen tahdissa (ketteryys).
- Tieto ei ole kenenkään käytettävissä (jatkuvuus).

Tietoriskien arvioinnissa tulee huomioida tiedon saatavuuteen, luottamuksellisuuteen, eheyteen, joustavuuteen ja jatkuvuuteen liittyvät riskit toimialan toiminnan mukaisesti. Oikean ihmisen tulee päästä oikeaan tietoon silloin, kun tietoa tarvitaan. Tieto voi olla saavuttamattomissa tai sitä ei löydy, kun sitä tarvitaan. Tieto voi vuotaa asiattomille. Tieto voi puuttua kokonaan tai olla puutteellista tai virheellistä. Tieto voi olla vaikeasti kehitettävissä tai laajennettavissa kehittyvän toiminnan tukemiseksi. Laaja teknologian toimintahäiriö voi aiheuttaa, ettei kukaan pääse käsittelemään tietoa.

Kaupungin toiminta on enenevässä määrin riippuvainen toimintaa ja fyysistä maailmaa ohjaavasta verkotetusta automaatioteknologiasta, jopa siinä määrin, että henkilöiden turvallisuus voi vaarantua. On syytä huomioida, että tietoon ja teknologiaan kohdistuva riski voi aiheuttaa vaikutuksen ihmisen terveyteen tai henkeen, jos tietojärjestelmä ohjaa fyysisen maailman toimintaa, josta ihmiset ovat riippuvaisia kuten esimerkiksi kiinteistönohjausjärjestelmät.

Tietosuojariskeihin varautumisessa tulee arvioida, aiheuttaako henkilötietojen käsittely luonnolliselle henkilölle (palveluidemme asiakkaille, henkilökunnalle ja sidosryhmien henkilöille) jonkin oikeuden tai vapauden menetyksen. Esimerkiksi arkaluonteisten tietojen vuotamisen tai virheellisten tietojen takia henkilö voi altistua syrjinnälle, menettää oikeuden palveluun (ei saa opiskelupaikkaa) tai saada virheellistä palvelua väärän päätöksen perusteella.

Tieto- ja tietosuojariskit voivat aiheutua tyypillisesti seuraavista syistä:

- Tietojen hallintatoimet ja käsittely on järjestetty puutteellisesti. Jos henkilötietojen käsittely on järjestetty puutteellisesti, henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen voi vaarantua.
- Tietoja ja tietojärjestelmiä voivat vaarantaa mm. laite-, ohjelma-, tietokanta- ja tietoliikenneviat sekä ympäristöriskit (esim. sähkökatko).
- Kaupungin henkilöstön tai ulkopuolisten henkilöiden tahattomat virheet tai tahallinen toiminta voi vaarantaa tiedon laadun tai tietojärjestelmien toimivuuden.
- Koska toimintaympäristöt ovat tyypillisesti verkotettuja, tietoturva ja tietosuoja voivat vaarantua tietojen siirrossa tai yhteyksien ja käyttöoikeuksien määrittelyssä (esim. henkilöstön tiedot jaetaan useisiin järjestelmiin)
- Tietoturva- ja tietosuojariskit ovat suurempia, kun tietoja käsitellään ja tietojärjestelmiä käytetään julkisten verkkojen kautta, työpaikan ulkopuolelta ja/tai muilla kuin kaupungin laitteilla. Silloin asiattomat voivat päästä helpommin tietoon käsiksi luvattomasti.

Kyberriskien arvioinnissa on olennaista toimintaa ohjaavien tietojärjestelmien kautta aiheutuvat fyysisen maailman vaikutukset. Anturit voivat tuottaa liikenteen ohjauksen, katujen kunnossapidon, talotekniikan, sairaaloiden, voimalaitosten ja vesihuoltolaitosten järjestelmiin erittäin suuria, jatkuvasti lisääntyviä tietomassoja, jotka voivat sisältää kaupungin kannalta kriittistä tietoa. Yhä useampia laitteita on kytketty toimintaympäristöissä toisiinsa. Näiden lisäksi kyberturva voi vaarantua sensorien tuottaminen tietojen tahattomasta tai tahallisesta vääristymisestä johtuen (esimerkiksi ilmastointijärjestelmän lämpötilasensorin häirintä laservalolla). Muita digitalisoinnin kyberuhkia ovat mm. robotisoinnin virheet, massatiedon hallinnan riskit ja toiminnan logiikan automatisoinnin virheiden nopeus. Lisäksi lainsäädännön muutoksia ei ehkä ehditä toteuttaa monimutkaisessa toimintaympäristössä riittävän nopeasti.

3.2 Riskienhallinnan toimenpiteet

Kun tietoturva- ja tietosuojavaatimukset on määritelty tietoriskien suuruuden mukaisesti, voidaan hallinnolliset ja tekniset suojaustoimenpiteet suunnitella ja toteuttaa optimaalisesti.

Hallinnollisia suojaustoimenpiteitä ovat mm. tietoturvan ja tietosuojan sisään rakentaminen osaksi kaupungin kaikkia prosesseja (esim. tietoturva- ja tietoturvavaatimukset osana hankintaprosessia) ja palveluja (esim. henkilöstön tukeminen häiriötilanteessa).

Tietosuojatoimenpiteet tulee dokumentoida, jotta kaupunki täyttää tietosuojasetuksen mukaisen osoitusvelvollisuuden.

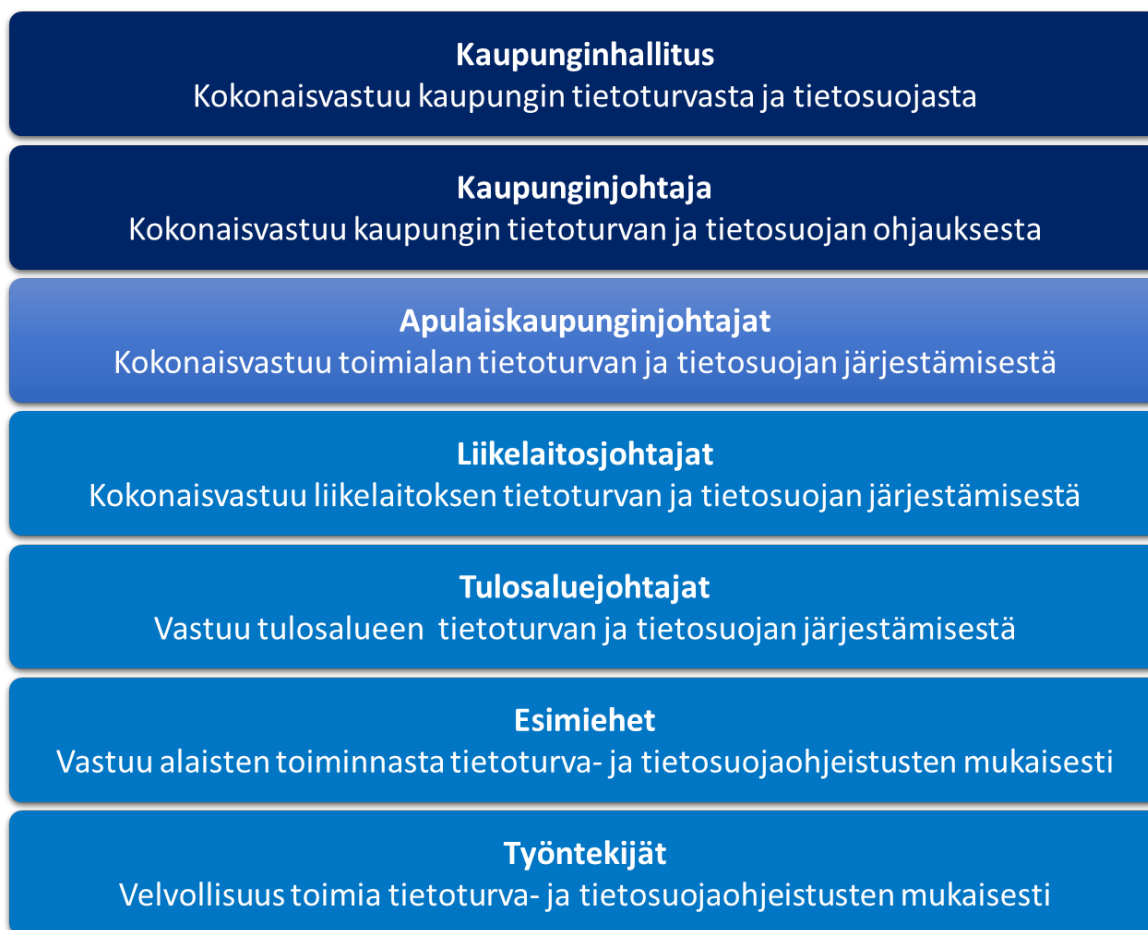
Teknisiä toimenpiteitä ovat mm. sekä teknisten suojausmekanismien sisään rakentaminen osaksi toiminta- ja tietotekniikkaa (esim. pääsykontrollit) että tietoturvatekniikan hyödyntäminen tiedon suojaamisessa (esim. lukko ja salausohjelma).

Parhaimmillaan tietoturva- ja tietosuojatoimenpiteet suojaavat tarpeen mukaan tietoa, mutta eivät hankaloita, hidasta tai jäykistä toimintaa, prosesseja tai tekniikkaa.

4 Tietoturvan ja tietosuojaan vastuut ja organisointi

Tietoturvan ja tietosuojaan vastuut on määritelty lyhyesti kaupungin hallintosäännössä. Tässä asiakirjassa syvennetään kaupungin viranhaltijoiden ja organisaatioiden tietoturva- ja tietoturvavastuita.

4.1 Tietoturvan ja tietosuojaan tilivelvollisuudet ja vastuut



Kuva 1 Yhteenveto Kaupungin tietoturva- ja tietosuojavastuista.

4.1.1 Kaupunginhallitus ja kaupunginjohtaja

Kaupunginhallitus huolehtii kuntalain perusteella kaupungin sisäisestä valvonnasta ja riskienhallinnan järjestämisestä, ja siten kaupunginhallituksella on kokonaisvastuu kaupungin tietoturvasta ja tietosuojasta. Kaupunginhallitus vastaa siitä, että kaupunki täyttää tietoturva- ja tietosuojalainsäädännön velvoitteet. Kaupunginhallitus hyväksyy kaupungin tietoturva- ja tietosuojapolitiikan.

Kaupunginjohtaja vastaa kaupungin tietoturvan ja tietosuojan ohjauksesta sekä vahvistaa niihin liittyvät kaupunkitasoiset päätökset.

Kaupunginhallituksen ja kaupunginjohtajan tulee sitoutua tietoturvan ja tietosuojan jatkuvaan kehittämiseen sekä huolehtia toiminnan riittävästä resursoinnista.

4.1.2 Apulaiskaupunginjohtajat

Apulaiskaupunginjohtajat vastaavat oman toimialansa tietoturvasta ja tietosuojasta. Apulaiskaupunginjohtajien tulee huolehtia riittävästä tietoturvan ja tietosuojan resursoinnista, ohjeistamisesta, koulutuksesta ja asioiden säännöllisestä käsittelystä johtoryhmissä toimialoillaan. Apulaiskaupunginjohtajat vahvistavat omia toimialojansa koskevat tietoturvan ja tietosuojan erityisohjeet. Toimialakohtaiset erityisohjeet voivat tarkentaa, täydentää ja tiukentaa kaupunkitasoisia ohjeistusta. Mikäli pakottavista syistä ilmenee tarve poiketa kaupunkitasoisesta ohjeistuksesta toimialakohtaisella erityisohjeistuksella, poikkeamia koskevat riskipäätökset tekee kaupunginjohtaja.

4.1.3 Vantaan tytäryhtiöiden ja liikelaitosten päättäjät

Vantaan kaupunkikonsernin tytäryhtiöiden ja liikelaitosten toimitusjohtajat, tytäryhtiöiden hallitukset ja liikelaitosten johtokunnat ovat vastuussa organisaationsa tietoturvan ja tietosuojan järjestämisestä voimassa olevan lainsäädännön sekä kaupungin tietoturva- ja tietosuojapolitiikan ja ohjeistusten mukaisesti.

Tytäryhtiöiden ja liikelaitosten päättäjät vastaavat organisaationsa tietoturvasta ja tietosuojasta. Päättäjien tulee huolehtia riittävästä resursoinnista, ohjeistamisesta ja koulutuksesta organisaatiossaan. Päättäjät vahvistavat omaa organisaatiota koskevat tietoturvan ja tietosuojan erityisohjeet. Tytäryhtiöiden ja liikelaitosten erityisohjeet voivat tarkentaa, täydentää ja tiukentaa kaupunkitasoisia ohjeistusta.

Mikäli pakottavista syistä ilmenee tarve poiketa kaupunkitasoisesta ohjeistuksesta organisaatiokohtaisella erityisohjeistuksella, poikkeamia koskevat riskipäätökset tekee organisaation hallitus. Poikkeamapäätöksistä tulee tiedottaa kaupungin tietoturvapäällikölle ja/tai tietosuojavastaavalle.

4.1.4 Tulosalueiden johtajat ja tulosityksiköiden päälliköt sekä muut esimiehet

Kaupungin tulosalueiden johtajat (mukaan lukien liikelaitokset) ja tulosityksiköiden päälliköt ovat vastuussa tietoturvasta ja tietosuojasta oman tulosalueensa ja tulosityksikkönsä osalta. Johtajien ja päälliköiden tulee järjestää riittävä resursointi tietoturvan ja tietosuojan toteutumiseksi omassa yksikössään.

Tulosalueiden ja -yksiköiden päälliköt ovat vastuussa palveluiden tuottamisesta siten, että palveluiden käyttäjät voivat toimia tietoturvallisesti ja käsitellä henkilötietoja lainmukaisesti.

Johtajien, päälliköiden ja esimiesten tulee huolehtia alaistensa ja ulkopuolisten konsulttien

- sitouttamisesta kaupungin salassa pidettävän tiedon ja henkilötietojen asianmukaiseen suojaamiseen
- perehdyttämisestä tietoturva- ja tietosuojavastuisiin
- annettujen tietoturva- ja tietosuojamääräysten ja -ohjeiden noudattamisesta
- pääsystä tarpeelliseen tietoon työsuhteen tai yhteistyön alkaessa
- työtehtävien muuttuessa valtuuksien muutoksista ja
- työsuhteen tai yhteistyön päättyessä tietoon pääsyn ja valtuuksien poistamisesta sekä tietojen siirtämisestä kaupungille

Kaikkien esimiesten on saatettava havaitsemansa tai tietoonsa saamat tietoturva- tai tietosuojarikkomukset viipymättä kaupungin tietoturvapäällikön, toimialan tietosuojavastaavan ja/tai kaupungin tietosuojavastaavan tietoon.

4.1.5 Kaupungin palveluiden päälliköt ja vastuulliset

Vantaan kaupungin tulosalue tai tulosityksikkö, joka tuottaa kaupungin palveluita kaupungin henkilöstölle, kaupungin toiminnoille tai asiakkaille, on kokonaisvastuussa palvelunsa tietoturvasta ja tietosuojasta riippumatta siitä, onko palvelun osana hankittu teknologiaa tai ulkoistettu palvelun osia palveluntoimittajille.

Kaupungin palveluissa tulee

- määritellä tietoturvaan ja tietosuojaan liittyvät hallinnolliset ja tekniset vaatimukset
- ottaa vaatimukset huomioon palvelun kehittämisessä ja
- toteuttaa ne noudattaen kaupungin tietoturva- ja tietosuojalinjauksia.

Kaupungin tietoturvapäälliköllä ja tietosuojavastaavalla tai heidän edustajallaan on tarvittaessa oikeus varmistua tarkastamalla palvelun tietoturvan ja tietosuojan riittävästä tasosta mukaan lukien ostetut tai ulkoistetut palveluiden osat.

4.1.6 Palveluntoimittajat

Vantaan kaupungin tulosalue tai tulosityksikkö, joka ostaa teknologiaa tai palveluja ulkopuoliselta palveluntoimittajalta/-tuottajalta, vastaa tietoturvasta ja tietosuojasta myös ostetun teknologian ja palveluiden osalta.

Palvelusopimuksessa tulee sopia tietoturvaan ja tietosuojaan liittyvistä vaatimuksista ja käytännön toteuttamistoimenpiteistä. Vantaan kaupungin palveluntoimittajien tai -tuottajien edellytetään noudattavan kaupungin tietoturva- ja tietosuojalinjauksia. Vantaan kaupungilla tulee olla oikeus varmistua toimittajan tietoturvan ja tietosuojan riittävästä tasosta.

Mikäli palveluntoimittaja tai -tuottaja käsittelee kaupungin omistamia tai hallinnoimia henkilötietoja tai muita tietoja, sen on osapuolten välisessä sopimuksessa sitouduttava noudattamaan voimassa olevaa tietoturva- ja tietosuojalainsäädäntöä, kaupungin tietoturva- ja tietosuojapolitiikkaa sekä soveltuvin osin tietoturvaan ja tietosuojaan liittyviä kaupungin ohjeita ja määräyksiä.

Vantaan kaupungin palveluntoimittajilta tai -tuottajilta edellytetään sopimuksessa säännöllistä raportointia tietoturvaan ja tietosuojaan vaikuttavista seikoista. Kaupungilla tai luotetulla kolmannella osapuolella tulee olla tarkastusoikeus kaupungille toimitettujen ratkaisujen ja palveluiden tietoturvan ja tietosuojan tasoon.

4.1.7 Tiedon omistajat

Tiedon omistaja on yksikkö, jonka toimintaan tiedot lähinnä liittyvät tai jonka toimintaa ne tukevat, ja joka käyttää niihin kuuluvaa määräysvaltaa.

Tiedon omistajan tulee varmistaa tiedon koko elinkaaren ajan, että

- kaikki tieto on luokiteltu (julkisuusarvon määrittely),
- tietoa käsitellään huolellisesti, ja
- tieto on asianmukaisesti suojattu.

Tiedon omistaja päättää lakien ja kaupungin ohjeistuksen mukaisesta tiedon luokittelusta sekä sisäisen ja salassa pidettävän tiedon jakamisesta kaupungin sisällä ja luovuttamisesta ulkopuolisille.

Tiedon luokittelua, käsittelyä ja suojaamista on käsitelty tarkemmin kaupungin tietojen luokittelun ja käsittelyn ohjeistuksessa (Katso *Kaupungin tietoturva- ja tietosuojaohjeistus*).

4.1.8 Henkilörekisterin pitäjät

Henkilörekisterin pitäjällä tarkoitetaan organisaatiota, jonka käyttöä varten henkilörekisteri perustetaan, ja jolla on oikeus päättää henkilörekisterin käytöstä tai jonka tehtäväksi henkilörekisterin pito on lailla säädetty.

Vantaalla henkilötiedon rekisterinpitäjä on

- kaupunginhallitus koko kaupunkia koskevan henkilörekisterin osalta ja
- toimialan lautakunta tai vastaava luottamuselin toimialakohtaisen henkilörekisterin osalta

Henkilörekisterin pitäjä vastaa henkilötietoon kohdistuvien uhkien riski- ja vaikutusarvioinneista sekä henkilötiedon suojaamisesta.

4.1.9 Tietojärjestelmien omistajat

Tietojärjestelmällä tarkoitetaan kaupungin toimintaa varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan ja ylläpidetään kaupungin tietoa tai asiakirjoja ja niissä olevia tietoja.

Tietojärjestelmän omistaja on yksikkö, jonka toimintaan tietojärjestelmä lähinnä liittyy tai jonka toimintaa se tukee, ja joka käyttää siihen kuuluvaa määräysvaltaa.

Omistaja nimeää tietojärjestelmälle vastuuhenkilön, jonka vastuulle asianomainen tietojärjestelmä kuuluu, ja joka käyttää siihen kuuluvaa määräysvaltaa. Tietojärjestelmän vastuuhenkilö varmistaa, että tietojärjestelmä on asianmukaisesti luokiteltu, hallittu ja suojattu tiedon luokittelun ja kaupungin ohjeiden mukaisesti ja resurssien rajoissa. Tietohallinnon tietoturva- ja tietosuojavastuut on määritelty kappaleessa 4.2.5.

Tietojärjestelmän vastuuhenkilön tulee ilmoittaa tarvittaessa tietoturvaan tai tietosuojaan liittyvistä uhkista, riskeistä tai suojauksien puutteista esimiehelleen, tietoturvapäällikölle tai tietosuojavastaavalle.

4.1.10 Työntekijöiden ja muiden tietoja käsittelevien vastuu

Jokainen Vantaan kaupungin omistamia tai hallinnoimia tietoja käsittelevä (esim. viranhaltijat, työntekijät, luottamushenkilöt sekä sopimus- ja yhteistyötahojen edustajat) on vastuussa tietoturvan ja tietosuojan toteutumisesta omissa tehtävissään.

Jokaisen on noudatettava Vantaan kaupungin

- tietoturva- ja tietosuojapolitiikkaa,
- tietoturva-, tietosuoja- ja salassapitositoumuksia,
- tietoturva- ja tietosuojaperiaatteita ja -ohjeita,
- palvelu- ja tietojärjestelmäkohtaisia tietoturva- ja tietosuojakäyttöohjeita

Jokaisen vastuulla on tietoturvaan tai tietosuojaan liittyvien uhkien, riskien tai rikkomusten ilmoittaminen viipymättä

- esimiehelleen,
- palvelusta tai toiminnasta vastuulliselle taholle (esim. palvelun tukeen tai tietojärjestelmän pääkäyttäjälle)
- tietoturva- tai tietosuojapoikkeamien ilmoituskanavaan tai
- tietoturvapäällikölle tai tietosuojavastaavalle.

4.2 Tietoturvan ja tietosuojan järjestäminen: tietoturvan ja tietosuojan hallinta, -palvelu ja -teknologia

Kuva 2. Yhteenvedo kaupungin tietoturvan ja tietosuojan järjestämisvastuista.



4.2.1 Tietoturvapäälikkö

Tietoturvapäälikkö vastaa

- tietoturvan kehittämishankkeiden valmistelusta ja ohjauksesta
- tietoturvaohjeistuksien valmistelusta ja jalkauttamisesta
- tietoturvatietouden edistämisestä
- tietoturvakoulutuksen tuottamisesta osaksi kaupungin koulutuksia
- tietoturvapalveluiden ohjauksesta
- tietoturvarikkomusten hallinnoinnista
- tietoturvan seurannasta, viestinnästä ja raportoinnista
- kaupunkia ohjaavan tietoturvasäätelyn seurannasta

Tietoturvapäälikkö raportoi säännöllisesti tietoturvasta kaupungin johdolle sekä tarvittaessa kaupungin eri toimielimille. Tietoturvapäälikön tukena toimii kaupungin tietoturva- ja tietosuojatyöryhmä.

4.2.2 Tietosuojavastaava

Tietosuojavastaava toimii Vantaan kaupungin kaupunkitasoisena tietosuojavastaavana. Toimiala voi tarpeen mukaan nimetä toimialakohtaisen tietosuojavastaavan, jonka tulee raportoida tietosuojasta myös kaupungin tietosuojavastaavalle.

Tietosuojavastaava vastaa

- tietosuojan kehittämishankkeiden valmistelusta ja ohjauksesta
- tietosuojaoheistuksien valmistelusta ja jalkauttamisesta

- tietosuojatietouden edistämisestä
- tietosuojakoulutuksen tuottamisesta osaksi kaupungin koulutuksia
- tietosuojapalveluiden ohjauksesta
- tietosuojarikkomusten hallinnoinnista
- henkilötietojen käsittelyn ohjauksesta ja seurannasta lainsäädännön, viranomaismääräysten sekä kaupungin ohjeistusten mukaisesti
- tietosuojan viestinnästä ja raportoinnista
- yhteydenpidosta ja yhteistyöstä rekisteröityjen ja valvontaviranomaisen kanssa
- kaupunkia ohjaavan tietosuojasääntelyn seurannasta

Tietosuojavastaava raportoi säännöllisesti tietosuojasta kaupungin johdolle sekä tarvittaessa kaupungin eri toimielimille. Tietosuojavastaavan tukena toimii kaupungin tietoturva- ja tietosuojatyöryhmä.

4.2.3 Tietoturva- ja tietosuojatyöryhmä

Työryhmän jäsenet toimivat yhteyshenkilöinä tietoturva- ja tietosuoja-asioissa työryhmän ja oman toimialansa välillä. Toimialajohtajat vastaavat oman toimialansa osalta yhteyshenkilöiden tehtävän hoitamisen edellyttämästä koulutuksesta ja työajan resursoinnista.

Työryhmän jäsenten tehtävänä on

- valmistella kaupunkia koskevia tietoturvaan ja tietosuojaan liittyviä ohjeita sekä antaa suosituksia ja kannanottoja edellä mainituista asioista
- viedä kaupungin tietoturva- ja tietosuojaohjeistuksia omalle toimialalle jalkautettavaksi
- tuoda työryhmän käsittelyyn toimialan ehdotuksia kaupungin tietoturvan ja tietosuojan parantamiseksi
- seurata kaupungin tietoturva- ja tietosuojaohjeistuksen toteutumista toimialallaan
- nostaa kaupunkia koskevia tietoturva- ja tietosuojapuutteita työryhmän käsittelyyn

4.2.4 Toimialojen tietoturva- ja/tai tietosuojavastaavat

Toimialalla voi olla nimetty toimialakohtainen tietoturva- ja/tai tietosuojavastaava.

Vastaavan tehtävänä on omalla toimialallaan

- laatia ja esittää toimialakohtainen käytännön ohjeistus
- opastaa, neuvoa ja jalkauttaa käytäntöjä
- seurata määräysten ja ohjeiden noudattamista
- raportoida toimialan johdolle ja kaupungin tietoturvapäällikölle ja/tai tietosuojavastaavalle.

Toimialalla voi olla oma pysyvä tai tilapäinen toimialakohtainen operatiivinen tietoturva- ja tietosuojatyöryhmä asioiden juoksevaan käsittelyyn.

4.2.5 Tietohallinnon palvelukeskus

Tietohallinto vastaa tietohallintojohtajan johdolla

- kaupungin IT-ympäristön ja tietojärjestelmien tietoturvan ja tietosuojan suunnittelusta, kehittämisestä ja toteuttamisesta sekä toteutumisen seuraamisesta
- kaupungin tietojärjestelmäpalveluiden tuottamisesta siten, että palveluiden käyttäjät voivat toimia tietoturvallisesti ja käsitellä henkilötietoja lainmukaisesti
- hallinnollisten ja teknisten keinojen tuottamisesta IT-ympäristössä ja tietojärjestelmissä olevan tiedon ja sen käsittelyn suojaamiseksi
- kaupungin IT-ympäristön ja tietojärjestelmien tietoturva- ja tietosuojaohjeistuksen tuottamisesta ja jalkauttamisesta
- IT-ympäristön tietoturvatietouden edistämisestä ja -koulutuksen tuottamisesta
- IT-ympäristöön ja tietojärjestelmiin kohdistuvien merkittävien uusien uhkatekijöiden raportoinnista kaupungin tietoturvapäällikölle
- tietoturva- ja tietosuoja-rikkomuksien raportoinnista viipymättä kaupungin tietoturvapäällikölle tai tietosuojavastaavalle.

4.2.6 Henkilöstökeskus

Henkilöstökeskuksen tulee varmistaa henkilöstön tietojen ajantasaisuus ja oikeellisuus sekä mahdollistaa kaupungin henkilöstön lainmukainen ja kaupungin tietosuojaohjeistuksen mukainen henkilötietojen käsittely.

4.2.7 Hankintakeskus ja hankinnoista vastaavat

Hankintakeskus vastaa hankinnan kohteen tietoturvan ja tietosuojan tavoitteiden ja vaatimuksien sisällyttämisestä osaksi hankintaprosessia.

Hankintakeskus vastaa siitä, että kilpailuttamisprosessissa toteutetaan hankinnan kohteeseen liittyvien tietoriskien arviointi ja niihin liittyvien suojaamisvaatimusten määrittely. Suojaamisvaatimusten määrittelyn sisältö tulee toteuttaa yhteistyössä hankintakeskuksen ja tietohallinnon kanssa. Hankintakeskus vastaa siitä, että tietoriskien seuranta koskeva toimintamalli sisällytetään hankintasopimuksiin, mutta seurannasta vastaa tietojärjestelmän tai tiedon omistaja.

Toimialojen hankinnoista vastaavien tulee ottaa huomioon tietoriskien mukaisesti tietoturva- ja tietosuojatavoitteet ja vaatimukset hankinnoissa, sopimuksissa ja toimittajien hallinnassa.

5 Tietoturvan ja tietosuojan seuranta, koulutus, ohjeet ja viestintä

Jokaisella Vantaan kaupungin toimintaympäristössä toimivalla on velvollisuus ilmoittaa havaitsemistaan tietoturva- ja tietosuojapuuutteista tai epäilemistään tietoturva- tai tietosuojarikkomuksista. Havainnoista tulee ilmoittaa esimiehelle tai muulle kaupungin työntekijälle. Vakavat tietoturva- ja tietosuojapuuutteet tulee saattaa viipymättä kaupungin tietoturvapäällikön ja tietosuojavastaavan tietoon.

Tietohallinnon tulee toteuttaa tietojärjestelmien suojaus lainsäädännön ja muiden määräysten ja suositusten edellyttämällä tavalla. Tietojärjestelmien käyttöä tulee lokittaa, valvoa ja seurata lainsäädännön mukaisesti. Tietohallinnon tulee puuttua tietoturva- ja tietosuojaloukkauksiin yhteistyössä tietoturva- ja/tai tietosuojahallinnan kanssa (kts. kuva 2 tietoturvan ja tietosuojan järjestäminen). Tietoturva- ja tietosuojahallinnan tulee seurata ja tarkastaa tietojen käsittelyn ja tietojärjestelmien tietoturvan ja tietosuojan tehokkuutta säännöllisesti.

Uusien työntekijöiden perehdyttämiseen kuuluu tietoturva- ja tietosuojaopastus sekä Vantaan kaupungin ja toimialakohtaisiin tietoturva- ja tietosuojaohjeisiin tutustuminen. Tietoturva- ja tietosuojahallinnan tulee pitää yllä henkilöstön tietoturva- ja tietosuojatietoisuutta säännöllisellä koulutuksella sekä ajantasaisilla ohjeilla ja tiedotuksella.

Tietohallintojohtaja, tietoturvapäällikkö ja tietosuojavastaava vastaavat yhteistyössä kaupungin johdon sekä viestinnän tulosalueen kanssa kaupungin tietoturva- ja tietosuojaviestinnästä. Kaupungin toimialat, liikelaitokset ja tytäryhteisöt vastaavat oman organisaationsa tiedottamisesta em. asioissa yhteistyössä kaupungin viestinnän kanssa.

6 Liite 1: Tietoturvan ja tietosuojaan käsitteitä

Käsitteiden määrittelyssä on käytetty lähteinä valtionhallinnon tietoturvaohjeistusta (VAHTI) ja EU:n tietosuoja-asetusta.

Asenne

Tietoturvan ja tietosuojaan tarpeen ja merkityksen ymmärtäminen sekä, motivoituminen ja sitoutuminen noudattamaan tietoturva- ja tietosuojaohjeita ja -määräyksiä.

Eheys

Eheys tarkoittaa tiedon ja tietojärjestelmän luotettavuutta sisäisen ristiriidattomuuden, kattavuuden, täydellisyyden, ajantasaisuuden, oikeellisuuden ja käyttökelpoisuuden kautta.

Eheys edellyttää tiedon ja tietojärjestelmän muutoksien todentamista kirjausketjusta (lokittamista) ja valtuudettomien muutoksien estämistä.

Fyysinen turvallisuus

Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartiointin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirien toimittamien tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen turvallisuus

Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilörekisteri

Henkilörekisteri on sähköinen tai paperimuotoinen rekisteri tai luettelo, johon on koottu samaa käyttötarkoitusta varten henkilötietoja.

Henkilöstöturvallisuus

Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhteisöjen järjestelyihin liittyvien turvatekijöiden hoitamista.

Jatkuvuussuunnittelu

Jatkuvuussuunnittelu tarkoittaa niitä toimia, joiden avulla pyritään pienentämään ja lyhentämään toimintaa häiritsevien tapahtumien vaikutusta ja kestoja. Se sisältää varajärjestelyitä sekä toimenpiteitä, jotka parantavat toimintaa häiriötilanteissa tai toipumista ongelmien jälkeen. Jatkuvuussuunnittelu sisältää myös suunnitelmat, joissa kuvataan johtaminen, vastuut ja toimenpiteet, joiden mukaan toimintoja voidaan jatkaa erilaisissa häiriötilanteissa.

Jäljitettävyys

Tarpeen tullen on selvitettävissä, mitä tiedolle tai tietojärjestelmälle on tehty, kuka toimenpiteen on tehnyt ja milloin se on tehty.

Kiistämättömyys

Kiistämättömyyttä tarvitaan tiedon alkuperän, luovutuksen ja käsittelytapahtumien sekä tietojärjestelmämuutoksien luotettavuuden varmentamiseen. Luotettava näyttö saavutetaan tietoteknisin menetelmin, että tietty henkilö on tehnyt tietyn tietotapahtuman tai järjestelmämuutoksen. Tietotapahtumiin (lähetys, vastaanotto, lukeminen, käsittely) ja tietojärjestelmämuutoksiin liitetään aikaleima, joka todistaa tapahtuman ajankohdan.

Käytettävyys

Tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla, helposti hyödynnettävissä, käytettävissä haluttuna aikana ja vaaditulla tavalla sekä ilman ylimääräistä vaivaa.

Kyberriski

Tarkoittaa toimintateknologian ja sähköisten palveluiden kautta epävarmuuden vaikutusta fyysiseen toimintaan, poikkeamaa toiminnassa. Vaikutus voi olla asiakaspalvelun saatavuuteen, tarkkuuteen, joustavuuteen tai jatkuvuuteen, joka aiheuttaa palvelua saavien ihmisten toiminnan keskeytymisen tai virheellisyyteen. Pahimmassa tapauksessa ihmiselle voi aiheutua pysyvä vamma tai hengen menetys esim. teknologiasabotaasin johdosta. Kts. Kyberturva.

Kyberturva

Kyberturvalla kaupunki pyrkii suojaamaan ihmisten tuottaman tiedon tai automaattisesti toimivien älykkäiden järjestelmien vaikutukset päätöksiin, toimintaan ja fyysiseen maailmaan kuten esimerkiksi taloushallinnon ja liikenteenohjauksen järjestelmät.

Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten palveluiden ja verkotettujen järjestelmien poikkeamien vaikutuksiin kaupungin toiminnoissa.

Kyberturvassa yhdistyy tietoturvan, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelu. Useat kaupungin toimialojen kriittiset toiminnot kuten rahaliikenne, energianjakelu, kaupungin infrastruktuuri, sivistystoimi sekä sosiaali- ja terveystoimi ovat riippuvaisia toimintoja automatisoitujen tietojärjestelmien ja -verkkojen luotettavuudesta ja toimivuudesta.

Kaupungin toimintoja tukeviin järjestelmiin ja verkkoihin kohdistuvat häiriöt muodostavat kyberuhan kaupungin asiakaspalveluille. Häiriöt voivat olla tahallisia verkkohyökkäyksiä tai tahattomia laitteistojen ja ohjelmistojen vikaantumisia.

Käyttöturvallisuus

Toimenpiteitä, joilla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käytön valvonnasta, ohjelmistotuesta ja varmistuksista.

Laitteistoturvallisuus

Laitteistojen käytettävyyden, toiminnan, ylläpidon sekä laitteiden ja tarvikkeiden saatavuuden turvaavat toimenpiteet

Laitteiston elinkaarta turvataan laitteistoturvallisuudella, johon kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Ohjelmistoturvallisuus

Käyttöjärjestelmiin, varus- ja työkaluohjelmistoihin sekä muihin ohjelmistoihin kohdistuvat turvatoimet. Näitä ovat esim. ohjelmistojen tunnistamis-, eheys-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus.

Luottamuksellisuus

Tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus. Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn, tietojärjestelmiin ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Palveluntoimittaja

Kaupungin julkisen tai sisäisen palvelu kokonaan tai osittain on sopimuksella ulkoistettu palveluntoimittajalle, jonka vastuulla on toimittaa palvelua tai sen osaa sopimuksella määrätyllä tavalla ja laadulla yhdessä kaupungin kanssa sovittujen hallintatoimien sekä jatkuvuuteen, tietoturvaan ja tietosuojaan liittyvien vaatimusten mukaisesti.

Palveluntuottaja

Kaupungin organisaation yksikkö tai sen johtaja, jonka vastuulla on kaupungin ulkoinen palvelu asiakkaille tai kaupungin sisäinen tukipalvelu henkilöstölle. Tyypillisesti palvelu on asianomaisen yksikön tai sen johtajan päätäntävallassa sekä kulut ja tuotot lasketaan yksikön talouteen. Joissain tapauksissa kaupungin sisäisessä käsitteiden käytössä käytetään käsitettä *palveluntuottaja* tarkoittaen yllämääriteltyä *palveluntoimittaja* käsitettä.

Pääsynvalvonta

Tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palveluelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille

Riski

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Saatavuus

Palvelu, tieto tai tietojärjestelmä on saatavilla ja käytettävissä, kun sitä tarvitaan. Helppokäyttöisyys, nopeus, joustavuus ja luotettavuus ovat saatavuuden eri näkökulmia.

Tiedon laatu

Tarkoittaa tiedon ominaisuuksia kuten tiedon täydellisyys (completeness), soveltuvuus (validity), johdonmukaisuus (consistency), ajanmukaisuus (timeliness) ja tarkkuus (accuracy), jotka yhdessä mahdollistavat tiedon käyttämisen tiettyä tarkoitusta varten. Kaikki edellämainitut tiedon laadun kriteerit yhdessä ovat ISO 9000:2015 standardin mukaan yleisesti pakollisia tiedon laadun varmistamisessa osana toiminnan laatua.

Tietoaineistoturvallisuus

Toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen saatavuuden, käytettävyyden, eheyden, jäljitettävyyden ja luottamuksellisuuden ylläpitämiseksi, keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietojärjestelmä

Ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt

Tietojärjestelmän omistaja

Vastaa mm. henkilötietolaissa mainitun rekisterinpitäjän velvollisuuksista sekä oman tietojärjestelmänsä tietoturvallisuudesta dokumentoinnin, turvaluokittelun, käyttöoikeusrekisterin ylläpidon, käyttöoikeuksien, käytön, varmistusten, tuen, koulutuksen, ylläpidon, kehittämisen ja jatkuvuussuunnittelun osalta.

Tietojärjestelmän pääkäyttäjä

Pääkäyttäjällä on laajat oikeudet hallinnoida tietyssä tietojärjestelmässä muiden käyttäjien käyttäjätunnuksia, laiteresursseja, tiedostoja ja järjestelmän suojauksia.

Tietojärjestelmäriski

Tarkoittaa epävarmuuden vaikutusta tietojärjestelmään, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna. Tyypillisiä vaikutuksia on tietojärjestelmän toimintavirhe tai -häiriö, joka aiheuttaa tietojärjestelmän käyttökatkoksen tai sen tuotoksien käyttökelvottomuuden tai virheellisuuden ja tietojärjestelmää käyttävien organisaatioiden toiminnan keskeytymisen tai virheellisuuden.

Tietojärjestelmien ja IT-ympäristön turvallisuus

Hallinnolliset toimet kuten ohjeistus, kehitys ja seuranta, joilla pyritään aikaansaamaan tietojärjestelmien ja IT-ympäristön turvallisuus. Tietojärjestelmien hallinnolliset ja tekniset suojaamisen ja turvaamisen toimenpiteet.

Tietojärjestelmien käytettävyyden, virheettömyyden ja luottamuksellisuuden hallinnollinen ja tekninen varmistaminen.

Tietojärjestelmien käyttöjärjestelmien ja ohjelmistojen tunnistaminen, valtuuttaminen ja eheyden varmistaminen ja tiedon tekninen suojaaminen.

Tietojärjestelmien käyttäjien todentamisen ja valtuutuksien tekninen toteutus.

Tietojärjestelmien jatkuvuuden varmistamisen toimenpiteet.

Tietoliikenneturvallisuus

Hallinnolliset toimet kuten ohjeistus, kehitys ja seuranta, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Tiedonsiirtoyhteyksien suojaamisen ja turvaamisen toimenpiteet. Tietoliikenneyhteyksien käytettävyyden, virheettömyyden ja luottamuksellisuuden tekninen varmistaminen. Laitteiden verkkoon kytkettyjen laitteiden tunnistamisen ja valtuutuksien toimenpiteet. Verkon jatkuvuuden varmistamisen toimenpiteet.

Tietoriski

Tarkoittaa epävarmuuden vaikutusta tietoon, poikkeamaa tiedossa. Vaikutus voi olla tiedon saatavuuteen, käyttökelpoisuuteen, oikeellisuuteen, eheyteen, joustavuuteen tai jatkuvuuteen, joka aiheuttaa tietoa käyttävien organisaatioiden toiminnan keskeytymisen tai virheellisyyden.

Tietosuoja

Tietosuojalla tarkoitetaan henkilötietojen ja erityisesti arkaluonteisten tietojen suojaamista asiattomalta käsittelyltä.

Henkilötiedolla tarkoitetaan kaikkia henkilöön liittyviä tietoja, joista tämä on tunnistettavissa.

- Henkilötietoja ovat mm. nimi, henkilötunnus, henkilöä esittävä valokuva, puhelinnumero, sähköpostiosoite, sijainti tai verkkotunniste (esim. IP-osoite).
- Arkaluonteisia henkilötietoja ovat mm. henkilön terveydentilaa, sairautta tai hoitotoimenpiteitä koskevat tiedot sekä tiedot henkilön saamista sosiaalihuollon palveluista ja etuuksista.

Tietosuojaloukkaus

Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Tietosuojariski

Tarkoittaa epävarmuuden vaikutusta henkilötietoon, poikkeamaa henkilötiedossa. Vaikutus voi olla henkilötiedon saatavuuteen, käyttökelpoisuuteen, oikeellisuuteen, eheyteen, joustavuuteen tai jatkuvuuteen, joka vaikuttaa luonnolliselle henkilölle (palveluidemme asiakkaille, henkilökunnalle ja sidosryhmien henkilöille) oikeuden tai vapauden menetyksen. Esimerkiksi arkaluonteisten henkilötietojen vuotaminen tai virheellisten henkilötietojen takia henkilö voi altistua syrjinnälle tai menettää oikeuden palveluun tai saada virheellistä palvelua.

Lisäksi henkilötietojen käsittely voi olla järjestetty puutteellisesti, siten että henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen vaarantuu.

Tietoturva

Tietoturvalla tarkoitetaan hallinnollisia, teknisiä ja muita mahdollisia keinoja, joilla suojataan ja varmennetaan kaupungin omistamaa tai hallinnoimaa tietoa ja sen käsittelyä kaikissa olosuhteissa. Tietoturvalla tavoitellaan asianmukaista tiedon suojaamista.

Tietoturva koskee digitaalisessa, suullisessa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, arkistointia, luovuttamista, siirtämistä ja hävittämistä.

Tietoturva muodostuu tiedon saatavuudesta, käytettävyydestä, eheydestä, luottamuksellisuudesta, kiistämättömyydestä, jäljitettävyydestä ja pääsynvalvonnasta sekä henkilöstön osaamisesta, resursseista, toimintatavoista ja asenteesta. Tiedon käyttö- ja käsittelyoikeudet määrittyvät henkilön työtehtävän ja roolin mukaisesti. Tiedon asianmukainen suojaaminen tulee toteutua koko tiedon elinkaaren ajan, jota on kuvattu tarkemmin kaupungin tiedonluokitteluohjeessa.

Tietoturva koostuu hallinnollisesta turvallisuudesta, henkilöstöturvallisuudesta, fyysisestä turvallisuudesta, tietoliikenneturvallisuudesta, käyttöturvallisuudesta, tietoaineistoturvallisuudesta sekä laitteisto- ja ohjelmistoturvallisuudesta.

Tietoturvallisuus

Järjestelyt, joilla pyritään varmistamaan tiedon turvallisuus. Katso tietoturva.

Tietoturvarikkomus

Lievät tietoturvarikkomukset ovat väärinkäytöksiä kuten esimerkiksi henkilökohtaisen tietoturvan laiminlyönti, epäasiallinen käytös, haitan aiheuttaminen, resurssien tuhlaus, haittaohjelmien torjunnan tai tietoturvapäivityksien laiminlyönti, luvaton kaupallinen tai poliittinen toiminta tai kulunvalvontasääntöjen rikkominen.

Tietoturvarikkomukset ovat vakavampia väärinkäytöksiä tai turvallisuuden vaarantamisia kuten esimerkiksi ohjelmien ja pelien luvaton kopiointi, luvattomien ohjelmien asentaminen, ylläpitäjän työkalujen luvaton hallussapito, palvelun luvaton pystytys, tunnuksen luovuttaminen tai tiedon suojaamisen vaarantaminen.

Vakavat tietoturvarikkomukset ovat lain mukaan rikkomuksena tai rikoksena tuomittavia tekoja kuten esimerkiksi luvaton hakkerointi ja tunkeutuminen, rikoslain alaisen materiaalin oikeudeton käsittely, tekijänoikeuslain alaisen materiaalin laiton levittäminen, tarkoituksellinen luvaton porttiskannaus, haittaohjelmien tahallinen levittäminen ja palvelunestohyökkäys.

Toipumissuunnittelu

Toipumissuunnittelu liittyy yleensä tietojärjestelmiin ja niiden toipumiseen häiriötilanteissa, ja se on tärkeä osa jatkuvuussuunnittelua. Yksittäinen toipumissuunnitelma määrittelee ja dokumentoi suunnitelman piirissä oleviin toimintoihin liittyville tietojärjestelmille käytännön toimenpiteet, roolit ja vastuut normaalitilaan palaamiseksi. Lisäksi toipumissuunnitelmassa kuvataan teknisesti korkean käytettävyyden vaatimat toteutustavat sekä miten häiriötilanteessa viestitään toipumista ohjaavalle taholle.

Toipumissuunnitelmat kuvaavat operatiivisella tasolla ja konkreettisesti järjestelmien palauttamisen häiriötilanteista. Ne sisältävät ohjeet vakavasta häiriöstä toipumiseen, normaaliin toimintaan paluusta ja toiminnan jatkamisesta. Jatkuvuussuunnitelma ohjaa toipumissuunnitelmien toteutusta.

Varautuminen

Varautumisella tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen kaikissa tilanteissa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset etukäteisvalmistelut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun.